CISCO ADVANCED MALWARE PROTECTION CASE STUDY

Georgetown University

Introduction

This case study of Georgetown University is based on a March 2017 survey of Cisco Advanced Malware Protection customers by TechValidate, a 3rd-party research service.

> "Deploying AMP for Endpoints alongside other AMP deployments has helped my organization uncover threats faster and improve overall security effectiveness."

Challenges

The business challenges that led the profiled organization to evaluate and ultimately select Cisco Advanced Malware Protection:

- Chose AMP for Endpoints for the following reasons:
  - Superior protection from advanced threats and hackers
  - Rapid time to detection of threats
  - Endpoint visibility into file activity and threats
  - Ability to continuously monitor file behavior
  - Retrospective alerting to uncover stealthy attacks
  - Ability to quickly understand the threat and what it's trying to do
  - Simple, easy to use management interface

Use Case

The key features and functionalities of Cisco Advanced Malware Protection that the surveyed organization uses:

- Deployed the following in addition to AMP for Endpoints:
  - AMP for Networks (AMP on Cisco Firepower NGIPS)
  - AMP for Firewall (AMP on a Cisco ASA or NGFW Firewall)

Results

The surveyed organization achieved the following results with Cisco Advanced Malware Protection:

- Was able to do the following with AMP for Endpoints:
  - Improve security effectiveness
  - Prevent breaches
  - Detect threats faster
  - Increase visibility into potential threats
  - Remediate advanced malware
  - Accelerate incident response
  - Reduce management complexity using Cisco AMP's integrated architecture
- Prevented / Detected / Defeated the following with AMP for Endpoints:
  - Advanced malware or advanced persistent threats (APTs)
  - Zero-day threats
  - Ransomware
  - Malvertising
  - Drive-by-attacks
  - Malicious email attachments
  - File-less or memory-only malware
- Reduced threat detection time by more than an hour with AMP for Endpoints.
- Experienced improvements in the following areas after deploying AMP for Endpoints:
  - Mean time to detection of previously unseen and/or unknown threats
  - Investigation speed and/or quality

Organization Profile

Organization:
Georgetown University

Industry:
Educational Institution

About Cisco Advanced Malware Protection

Get global threat intelligence, advanced sandboxing, and real-time malware blocking to prevent breaches with Cisco Advanced Malware Protection (AMP). But because you can't rely on prevention alone, AMP also continuously analyzes file activity across your extended network, so you can quickly detect, contain, and remove advanced malware.

Learn More:

Cisco

Cisco Advanced Malware Protection

Source: Nadim Elias El-Khoury, IT Director, Georgetown University

✓ Validated Published: Jul. 21, 2017 TVID: B3C-2DB-437

Research by TechValidate by SurveyMonkey